S03P1112 US00

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　９月２４日

出願番号
Application Number: 特願２００２－２７７６６１

[ST.10/C]: [ＪＰ２００２－２７７６６１]

出願人
Applicant(s): ソニー株式会社

２００３年　６月２７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５０９９４

【書類名】　特許願
【整理番号】　0290531903
【提出日】　平成14年 9月24日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　中野　雄彦
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭
【選任した代理人】
【識別番号】　100101801
【弁理士】
【氏名又は名称】　山田　英治
【選任した代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【手数料の表示】
【予納台帳番号】　048747
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　コンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

所定の使用条件下でコンテンツの使用を制御するコンテンツ使用制御装置であって、

コンテンツの使用を要求する他の装置又はユーザの識別用情報を取得する取得手段と、

他の装置又はユーザから取得した識別用情報を登録する登録手段と、

他の装置又はユーザからのコンテンツの使用要求に応答して、該要求元の識別用情報の登録の有無により使用の可否を決定する使用制御手段と、

を具備することを特徴とするコンテンツ使用制御装置。

【請求項２】

前記登録手段は他の装置又はユーザからの要求に応じて登録処理を行なう、

ことを特徴とする請求項１に記載のコンテンツ使用制御装置。

【請求項３】

前記登録手段は所定の登録可能数に余裕がある場合のみ新規の登録処理を行なう、

ことを特徴とする請求項１に記載のコンテンツ使用制御装置。

【請求項４】

前記登録手段は、他の装置又はユーザの識別用情報とともに登録済みの識別情報を持つクライアントに対するサービス提供を制御するための無効フラグを保持し、

前記使用制御手段は、無効フラグが設定されている他の装置又はユーザによるコンテンツの使用を制限する、

ことを特徴とする請求項１に記載のコンテンツ使用制御装置。

【請求項５】

前記登録手段における登録内容の変更を制限する変更制限手段をさらに備える

ことを特徴とする請求項１に記載のコンテンツ使用制御装置。

【請求項６】

前記変更制限手段は、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える回数を所定数に制限する、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項７】

前記変更制限手段は、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える頻度を制限する、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項８】

前記変更制限手段は、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える際に、該他の装置又はユーザに対して所定の操作を要求する、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項９】

前記変更制限手段は、登録済みの識別用情報の置き換えに際して、他の装置又は管理者から変更許諾情報を得ることを要求する、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項１０】

前記変更制限手段は、変更制限回数に応じた課金処理を行なう、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項１１】

前記変更制限手段は、登録の制限内容の変更に際して、他の装置又は所定の管理者から変更許諾情報を得ることを求める、

ことを特徴とする請求項５に記載のコンテンツ使用制御装置。

【請求項１２】

所定の使用条件下でコンテンツの使用を制御するコンテンツ使用制御方法であって、

コンテンツの使用を要求する他の装置又はユーザの識別用情報を取得する取得

ステップと、

他の装置又はユーザから取得した識別用情報を登録する登録ステップと、

他の装置又はユーザからのコンテンツの使用要求に応答して、該要求元の識別用情報の登録の有無により使用の可否を決定する使用制御ステップと、

を具備することを特徴とするコンテンツ使用制御方法。

【請求項１３】

前記登録ステップでは他の装置又はユーザからの要求に応じて登録処理を行なう、

ことを特徴とする請求項１２に記載のコンテンツ使用制御方法。

【請求項１４】

前記登録ステップでは所定の登録可能数に余裕がある場合のみ新規の登録処理を行なう、

ことを特徴とする請求項１２に記載のコンテンツ使用制御方法。

【請求項１５】

前記登録ステップでは、他の装置又はユーザの識別用情報とともに登録済みの識別情報を持つクライアントに対するサービス提供を制御するための無効フラグを保持し、

前記使用制御ステップでは、無効フラグが設定されている他の装置又はユーザによるコンテンツの使用を制限する、

ことを特徴とする請求項１２に記載のコンテンツ使用制御方法。

【請求項１６】

前記登録ステップにおける登録内容の変更を制限する変更制限ステップをさらに備える、

ことを特徴とする請求項１２に記載のコンテンツ使用制御方法。

【請求項１７】

前記変更制限ステップでは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える回数を所定数に制限する、

ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項１８】

前記変更制限ステップでは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える頻度を制限する、
ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項１９】

前記変更制限ステップでは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える際に、該他の装置又はユーザに対して所定の操作を要求する、ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項２０】

前記変更制限ステップでは、登録済みの識別用情報の置き換えに際して、他の装置又は管理者から変更許諾情報を得ることを要求する、
ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項２１】

前記変更制限ステップでは、変更制限回数に応じた課金処理を行なう、
ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項２２】

前記変更制限ステップでは、登録の制限内容の変更に際して、他の装置又は所定の管理者から変更許諾情報を得ることを求める、
ことを特徴とする請求項１６に記載のコンテンツ使用制御方法。

【請求項２３】

所定の使用条件下でコンテンツの使用を制御するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

コンテンツの使用を要求する他の装置又はユーザの識別用情報を取得する取得ステップと、

他の装置又はユーザから取得した識別用情報を登録する登録ステップと、

他の装置又はユーザからのコンテンツの使用要求に応答して、該要求元の識別用情報の登録の有無により使用の可否を決定する使用制御ステップと、
を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、所定の使用条件下でコンテンツの使用を制御するコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムに係り、特に、ネットワークなどを経由してユーザに提供されるコンテンツの使用を制御するコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムに関する。

【０００２】

さらに詳しくは、本発明は、ネットワークなどを経由して取得されたコンテンツに関する使用を特定のサーバ管理者の下で制御するコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムに係り、特に、エンドユーザの管理下に置かれるコンテンツの不正な使用を制御するコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムに関する。

【０００３】

【従来の技術】

現在、情報処理や情報通信などのコンピューティング技術が飛躍的に向上し、コンピュータ・システムが広汎に普及してきている。さらに、コンピュータどうしを相互接続するネットワーク・コンピューティング技術に対する要望も高まってきている。ネットワーク接続環境下では、コンピュータ資源の共有手複数ユーザ間で協働的作業を行なったり、情報コンテンツの共有・流通・配布・交換などを円滑に行なったりすることができる。

【０００４】

昨今では、インターネット利用の普及や、ブロードバンドなどの高速アクセス技術の進歩と低価格化により、多くのユーザが通信によって世界中で多様な情報コンテンツを簡単に伝送できるようになってきている。

【０００５】

一方、このような環境を利用し、映画や音楽などの著作物のデータを不正にコピー及び配信するシステム、例えばＮａｐｓｔｅｒ，　Ｇｎｕｔｅｌｌａなどが

登場し、コンテンツ保護に関する問題が発生している。ネットワークの規模や性能は今後さらに高まってくると推測されるが、このようなコンテンツの不正目的での利用を防ぐ手立て無しには、伝送できる情報が限定されてしまい、ネットワークの価値を有効に享受できなくなるおそれがある。また、コンテンツ不正利用が横行すると、コンテンツの制作・提供者側の意欲が減退し、業界全体の発展を阻害しかねない。

【０００６】

一般に、インターネットなどの広域ネットワークを経由してコンテンツを配信する場合、あらかじめユーザを登録又は課金処理して、正当な利用が確保されたときのみコンテンツを配信することにより、コンテンツを技術的に保護することができる。

【０００７】

ところが、最近では、ホーム・ネットワークなどプライベートなネットワークが浸透してきており、著作権法上の正当な使用の範囲で、ユーザは家庭内配信を行なうことができる。例えば、ＢＳデジタルを介して取得したコンテンツを、ｉ－Ｌｉｎｋなどで接続された情報機器同士で配信する。このような場合、末端のユーザにおいてコンテンツの保護を行なわなければならないが、独自にユーザの登録管理し、家庭内を越えてコンテンツの配信が無制限に行なわれるという危険がある。

【０００８】

したがって、ユーザが購入した映画や音楽などのコンテンツをホーム・サーバに格納し、インターネット経由で伝送・視聴するようなシステムでは、私的利用を超えるようなアクセスを防ぐ仕組みが必要になる。

【０００９】

現時点では、著作権保持者が認める標準化された方式は存在せず、米国では放送記録装置のインターネットによるコンテンツ伝送機能に関して訴訟が発生するなどの混乱が発生している。

【００１０】

私的利用を超えるような利用を防ぐ手立てとしては、サービスを利用できる機

器数を限定する、あるいはクライアント識別情報（例：ＭＡＣアドレス）を登録し、未登録クライアントからのアクセスを防止するなどの方法が既に存在する。しかしながら、これらはサーバ管理者が正しく設定し、故意に不正アクセスを可能にしない場合に有効なものである。コンテンツの権利者としては、サーバ管理者、特にホーム・サーバのようにエンドユーザが管理者となる場合でも、不正流通をある程度防ぐことが必要であると思料するが、このような要求を満たすような標準化された方式はまだ無い。

【００１１】

【発明が解決しようとする課題】

本発明の目的は、ネットワークなどを経由して取得されたコンテンツに関する使用を特定のサーバ管理者の下で制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することにある。

【００１２】

本発明のさらなる目的は、エンドユーザの管理下に置かれるコンテンツの不正な使用を制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することにある。

【００１３】

本発明のさらなる目的は、コンテンツがホーム・ネットワークなどのエンドユーザの管理下に置かれる際に、所定の使用条件を越えて無制限にコンテンツが配信・流通されることがないように制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することにある。

【００１４】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、所定の使用条件下でコンテンツの使用を制御するコンテンツ使用制御装置又はコンテンツ使用制御装置であって、

コンテンツの使用を要求する他の装置又はユーザの識別用情報を取得する取得

手段又はステップと、

他の装置又はユーザから取得した識別用情報を登録する登録手段又はステップと、

他の装置又はユーザからのコンテンツの使用要求に応答して、該要求元の識別用情報の登録の有無により使用の可否を決定する使用制御手段又はステップと、を具備することを特徴とするコンテンツ使用制御装置又はコンテンツ使用制御装置である。

【００１５】

本発明は、例えば映画や音楽などの有料コンテンツを出力可能な装置が、そのコンテンツの利用者を制限することで、そのコンテンツの利用権限を持たないユーザによる不正利用を防ぐのに有効である。すなわち、本発明に係るコンテンツ使用制御装置又はコンテンツ使用制限方法によれば、その提供サービスの利用に先立って利用する装置又はユーザの識別情報を登録する必要がある。これにより、登録ができない装置及びユーザによる不正利用を排除することができる。

【００１６】

ここで、前記登録手段又はステップは他の装置又はユーザからの要求に応じて登録処理を行なうようにしてもよい。

【００１７】

前記登録手段又はステップは所定の登録可能数に余裕がある場合のみ新規の登録処理を行なうようにしてもよい。このように登録可能数に制限を与えることにより、ユーザ登録が無制限に行なわれコンテンツが不正に配布・流通されるという事態を防止することができる。

【００１８】

また、前記登録手段又はステップは、他の装置又はユーザの識別用情報とともに登録済みの識別情報を持つクライアントに対するサービス提供を制御するための無効フラグを保持し、前記使用制御手段又はステップは、無効フラグが設定されている他の装置又はユーザによるコンテンツの使用を制限するようにしてもよい。

【００１９】

また、本発明の第１の側面に係るコンテンツ使用制限装置又はコンテンツ使用制限方法は、前記登録手段における登録内容の変更を制限する変更制限手段をさらに備えていてもよい。

【００２０】

登録情報データベースの登録内容の変更を無制限に許容すると、家庭内（著作権の保護範囲内）を越えてコンテンツの配布や流通が行なわれる危険がある。そこで、本発明に係るコンテンツ使用制御装置又はコンテンツ使用制御方法は、登録情報データベースに一旦登録した識別情報、すなわちサービスを利用できる他の機器やユーザを別のものに置き換えるような登録内容の変更手続きを制限することができる。

【００２１】

また、コンテンツ使用制御装置のユーザが故意にサービスの利用権限のない装置又はユーザを登録しても、その変更は制限されているため、無制限な不正利用はできない。また、他ユーザやその装置を登録してしまうと、自身や家族による利用を妨げる可能性があることから、変更の制限は不正登録を抑制する効果も期待できる。

【００２２】

一方、このようにサービスの利用制限を設けることで、無制限な不正利用を防止できるため、コンテンツ提供者の要求を十分満たすこととなり、さまざまなサービス、コンテンツが利用できるようになることが期待される。

【００２３】

ここで、前記変更制限手段又はステップは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える回数を所定数に制限するようにしてもよい。所定回数の変更を行なった後は、さらなる変更を禁止する。なお、変更可能回数はエンドユーザが改竄できないように保護されるものとする。

【００２４】

また、前記変更制限手段又はステップは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える頻度を制限するようにしてもよい。例えば、最後に登録内容の変更を行なってから所定時間が経過するまでは再度の変更を禁

止したり、所定時間内の変更回数を制限したりする。

【００２５】

また、前記変更制限手段又はステップは、登録済みの識別用情報を他の装置又はユーザの識別用情報に置き換える際に、該他の装置又はユーザに対して所定の操作を要求するようにしてもよい。例えば、パスワードの入力、所定のボタン押下操作（例えば、幾つかのボタンを決められた順序で押す）などである。

【００２６】

また、前記変更制限手段又はステップは、登録済みの識別用情報の置き換えに際して、他の装置又は管理者から変更許諾情報を得ることを要求するようにしてもよい。例えば、パスワードや鍵データを電話、インターネット、郵便、記録媒体、口頭などによって得て、直接又は間接的に装置がそれを確認した段階で変更を可能にする。

【００２７】

また、前記変更制限手段又はステップは、変更制限回数に応じた課金処理を行なうようにしてもよい。

【００２８】

また、前記変更制限手段又はステップは、登録の制限内容の変更に際して、他の装置又は所定の管理者から変更許諾情報を得ることを求めるようにしてもよい。例えば、パスワードや鍵データを電話、インターネット、郵便、記録媒体、口頭などによって得て、直接又は間接的に装置がそれを確認した段階で変更を可能にする。

【００２９】

また、登録済み情報の置き換え制限を変えられるようにすることで、エンドユーザが不都合を感じないレベルに制限を緩和するオプションを得ることが可能になるとともに、サービスやコンテンツの権利者は潜在的な不正利用可能範囲をコントロールすることができる。

【００３０】

また、本発明の第２の側面は、所定の使用条件下でコンテンツの使用を制御するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形

式で記述されたコンピュータ・プログラムであって、

コンテンツの使用を要求する他の装置又はユーザの識別用情報を取得する取得ステップと、

他の装置又はユーザから取得した識別用情報を登録する登録ステップと、

他の装置又はユーザからのコンテンツの使用要求に応答して、該要求元の識別用情報の登録の有無により使用の可否を決定する使用制御ステップと、

を具備することを特徴とするコンピュータ・プログラムである。

【００３１】

本発明の第２の側面に係るコンピュータ･プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第２の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第１の側面に係る視点自由形画像表示装置又はその方法と同様の作用効果を得ることができる。

【００３２】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３３】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

【００３４】

図１には、本発明の実施に供されるコンテンツ使用制御装置１００の基本構成を模式的に示している。

【００３５】

コンテンツ使用制御装置１００は、メイン・コントローラとしてのＣＰＵ（Central Processing Unit）１０１がオペレーティング・システム（ＯＳ）が提供するプログラム実行環境下で所定のプログラム・コードを実行するという形態で動作する。ＣＰＵ１０１は、バスを介して他の機器と相互接続されている。

【００３６】

本実施形態では、ＣＰＵ１０１は、所定の使用条件の下でコンテンツの提供（配布・流通など）を制御したり、コンテンツ提供先の登録や登録内容の変更を制限したりするためのコンテンツ使用制限アプリケーションを実行する。

【００３７】

記憶部１０２は、例えばＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）などの半導体メモリや、ハード・ディスク装置やＣＤ／ＤＶＤ読み書き装置などの外部記憶装置などで構成される。

【００３８】

ＲＡＭは、ＣＰＵ１０１において実行されるプログラム･コードをロードしたり、実行プログラムの作業データを一時保管したりするために使用される。本実施形態では、所定の使用条件の下でコンテンツの提供（配布・流通など）を制御したり、コンテンツ提供先の登録や登録内容の変更を制限したりするためのコンテンツ使用制限アプリケーションがＲＡＭ上にロードされる。

【００３９】

ＲＯＭは、データを恒久的に格納する半導体メモリであり、例えば、起動時の自己診断テスト（ＰＯＳＴ：Power On Self Test）や、ハードウェア入出力用のプログラム・コード（ＢＩＯＳ：Basic Input/Output System）などが書き込まれている。

【００４０】

ハード・ディスク装置は、記憶担体としての磁気ディスクを固定的に搭載した外部記憶装置であり（周知）、記憶容量やデータ転送速度などの点で他の外部記憶装置よりも優れている。ソフトウェア・プログラムを実行可能な状態でハード・ディスク装置に置くことを、プログラムのシステムへの「インストール」と呼ぶ。通常、ハード・ディスク装置には、ＣＰＵ１０１が実行すべきオペレーティング･システムのプログラム･コードや、アプリケーション･プログラム、デバイス･ドライバなどが不揮発的に格納されている。例えば、所定の使用条件の下でコンテンツの提供（配布・流通など）を制御したり、コンテンツ提供先の登録や登録内容の変更を制限したりするためのコンテンツ使用制限アプリケーションを

ハード・ディスク装置上にインストールすることができる。また、提供すべきコンテンツや、コンテンツ使用制限アプリケーションによって登録並びに登録内容の変更が行なわれるコンテンツ提供先の情報をハード・ディスク装置上に蓄積しておいてもよい。

【００４１】

ＣＤ／ＤＶＤ読み書き装置は、ＣＤ－ＲＯＭやＣＤ－Ｒ、ＤＶＤなどの可搬型メディアを装填して、そのデータ記録面にアクセスするための装置である。可搬型メディアは、主として、ソフトウェア･プログラムやデータ･ファイルなどをコンピュータ可読形式のデータとしてバックアップすることや、これらをシステム間で移動（すなわち販売･流通･配布を含む）する目的で使用される。例えば、所定の使用条件の下でコンテンツの提供（配布・流通など）を制御したり、コンテンツ提供先の登録や登録内容の変更を制限したりするためのコンテンツ使用制限アプリケーションなどを、これら可搬型メディアを利用して複数の機器間で物理的に流通・配布することができる。また、提供すべきコンテンツや、コンテンツ使用制限アプリケーションによって登録並びに登録内容の変更が行なわれるコンテンツ提供先の情報などを他の装置との間で交換するために、可搬型メディアを利用することができる。

【００４２】

出力部１０３は、ディスプレイやスピーカ、プリンタなどのユーザ出力装置（図示しない）、他の装置にコンテンツやその他の情報を送信する通信インターフェースなどで構成され、他の装置（クライアント）やユーザにコンテンツなどの所定サービスの提供を行なうために使用される。また、コンテンツのコンテンツ提供先となる他の装置やユーザの登録処理や所定のサービスの利用要求に応じられない場合にその情報を提示するために、出力部１０３を用いることができる。

【００４３】

入力部１０４は、他の装置（クライアント）やユーザから登録要求と所定サービスの利用要求を受けるとともに、他の装置やユーザの識別情報を得るのに使用される。また、登録内容や登録制限の変更操作も、入力部１０４を介して行なわれる。入力部１０４は、具体的には、通信インターフェースや、キーボードやマ

ウスなどのユーザ入力装置（図示しない）、あるいはユーザ要求や識別情報を受容可能なスイッチ、センサ、カメラなどで構成される。

【００４４】

所定の使用条件の下でコンテンツの提供（配布・流通など）を制御したり、コンテンツ提供先の登録や登録内容の変更を制限したりするためのコンテンツ使用制限アプリケーションを当該装置１００にダウンロードしたり、コンテンツ使用制限アプリケーションによって登録並びに登録内容の変更が行なわれるコンテンツ提供先の情報などを他の装置との間で交換するために、通信インターフェースを用いることができる。

【００４５】

なお、図１に示すようなコンテンツ使用制御装置１００の一例は、米ＩＢＭ社のパーソナル･コンピュータ”ＰＣ／ＡＴ（Personal Computer/Advanced Technology）”の互換機又は後継機である。勿論、他のアーキテクチャで構成されるコンピュータを、本実施形態に係るコンテンツ使用制御装置１００として適用することも可能である。その他の例としては、ハード・ディスク装置を伴う放送受信機が挙げられる。このように、コンテンツ使用制御装置１００自体がコンテンツを保持し、他の装置やユーザにコンテンツを供給する機能も同時に備える場合も考えられる。

【００４６】

コンテンツ使用制御装置１００が提供する所定サービスを利用する他の装置やユーザは、まず、当該装置１００にその識別情報の登録を要求する。これに対し、コンテンツ使用制御装置１００は、登録数や登録変更の制限に抵触しないかどうかを確認して、登録可能であれば登録処理を行なう。このように登録可能数や登録変更に制限を与えることにより、ユーザ登録や登録ユーザの変更が無制限に行なわれコンテンツが不正に配布・流通されるという事態を防止することができる。

【００４７】

図２には、コンテンツ使用制御装置１００（サーバ）が他の装置やユーザ（クライアント）に対して行なう登録処理シーケンスを示している。

【００４８】

クライアントは登録時に、サーバに対して自身の識別情報を伴う登録要求を送る。これを受けたサーバは、登録処理を起動し、その結果情報をクライアントに対して応答として送る。

【００４９】

また、図３には、コンテンツ使用制御装置１００上で実行される登録処理の手順をフローチャートの形式で示している。この処理手順は、実際にはＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００５０】

まず、要求元クライアントが既に登録済みかを確認し（ステップＳ１）、そうであれば登録は不要なので成功終了する。

【００５１】

一方、要求元が未登録の場合には、コンテンツ使用制御装置１００に課されている登録可能数を参照して、新規登録が可能かをさらに確認し（ステップＳ２）、可能なら登録処理を行ない、成功終了する。

【００５２】

新規登録が不可能の場合には、コンテンツ使用制御装置１００に課されている登録変更の制限内容を参照して、既に登録されているものの置き換えが可能かを確認し（ステップＳ３）、不可の場合は本処理ルーチンを失敗終了する（ステップＳ８）。

【００５３】

また、登録内容の置き換えが可能な場合は、そのために所定の処理が必要かどうかを確認する（ステップＳ４）。特に処理が不要なら何も行わず、必要ならその処理を経て（ステップＳ５）、登録内容の置換登録処理を行ない（ステップＳ６）、本処理ルーチンを成功終了する（ステップＳ７）。

【００５４】

コンテンツ使用制御装置１００が提供する所定サービスを利用したい他の装置やユーザは、当該装置１００に所定サービスを求める。これに対し、コンテンツ使用制御装置１００は、要求元の装置やユーザの識別情報が登録されているかど

うかを確認し、登録されていれば所定サービスを提供し、登録されていない場合には提供しない。

【００５５】

図４には、サーバとしてのコンテンツ使用制御装置１００に対して他の装置やユーザ（クライアント）がサービス要求を行なうための動作シーケンスを示している。

【００５６】

クライアントは、サービス利用時に、サーバに対して自身の識別情報を伴うサービス要求を送る。これを受けたサーバは、サービス可否判定処理を起動し、その結果情報をクライアントに対して応答として送る。そして、サービス可能な場合、サーバはクライアントにサービスを供給する。

【００５７】

図５には、コンテンツ使用制御装置１００がサービス提供に際して行なうサービス可否判定処理の手順をフローチャートの形式で示している。この処理手順は、実際にはＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００５８】

まず、サービス利用の要求元が送ってきた識別情報が、登録されているかどうかを確認する（ステップＳ１１）。

【００５９】

そして、登録済ならサービス提供が可能であると判断して（ステップＳ１２）、本処理ルーチンを成功終了するが、未登録ならサービス提供が不可と判断して（ステップＳ１３）、本処理ルーチンを失敗終了する。

【００６０】

また、図６には、図２及び図３を参照しながら説明したような登録シーケンスに相当する前処理を省略して、サービス要求シーケンス内でクライアントの登録処理まで行なうようにした場合の動作シーケンスを示している。

【００６１】

クライアントは、サービス利用時に、サーバに対して自身の識別情報を伴うサ

ービス要求を送る。

【００６２】

これを受けたサーバは、登録処理を起動し、引き続いて、サービス可否判定処理を起動し、その結果情報をクライアントに対して応答として送る。そして、サービス可能な場合、サーバはクライアントにサービスを供給する。

【００６３】

サーバ上で起動される登録処理並びにサービス可否判定処理の手順はそれぞれ図３及び図５に示したフローチャートと同様なので、ここでは説明を省略する。

【００６４】

図７には、サーバとしてのコンテンツ使用制御装置１００が保持する登録情報データベースの構成例を示している。

【００６５】

新規登録可能数というフィールドには、他の装置又はユーザの識別情報をあと幾つだけ新規登録できるかを示す値が書き込まれる。最大でｎ個の登録が可能な場合は、初期値がｎで、１つ登録する度に１ずつ値が減らされ、ｎ個の登録後には０になる。図３に示したフローチャートのステップＳ２で登録可能数に余裕があるかを確認する際に、この値が０でないかどうかが参照される。なお、一旦登録したものを変更登録する際には、この値は変えない。

【００６６】

クライアント識別情報というフィールドには、登録したクライアントの識別情報が格納される。図３に示したフローチャートのステップＳ１、並びに図５に示したフローチャートのステップＳ１１においてクライアントが登録済かを確認するときには、ここに格納された情報が参照され、登録要求元又はサービス利用要求元の識別情報と比較される。また、図３の登録処理では、新規登録時は未登録エリアに識別情報が格納され、登録変更時は既に登録されたエリアに新しい識別情報を上書きする。

【００６７】

無効フラグというフィールドは、登録済みの識別情報を持つクライアントに対するサービス提供を制御するための情報である。例えば、このフラグの値が０で

サービス不許可、１でサービス許可といった使い方をする。

【００６８】

上述の登録情報データベースの登録内容の変更を無制限に許容すると、家庭内（著作権の保護範囲内）を越えてコンテンツの配布や流通が行なわれる危険がある。そこで、本実施形態に係るコンテンツ使用制御装置１００は、登録情報データベースに一旦登録した識別情報、すなわちサービスを利用できる他の機器やユーザを別のものに置き換えるような登録内容の変更手続きを制限することができる。登録変更の制限方法の具体例について以下に説明する。

【００６９】

具体例（１）

登録済みの識別用情報を、別の装置又はユーザの識別用情報に置き換える回数を所定の数に制限する。所定回数の変更を行なった後は、さらなる変更を禁止する。

【００７０】

変更可能回数をあらかじめ所定の値として設定し、これを記憶部１０２などの不揮発の書き換え可能メモリ（ＮＶＲＡＭ、ＥＥＰＲＯＭ、ＨＤＤなど）に保持しておく。そして、図３に示したフローチャートのステップＳ３における変更可能確認の処理では、この保持されている値を参照すればよい。

【００７１】

図８には、登録内容の変更可能確認の処理手順をフローチャートの形式で示している。この処理手順は、実際には、ＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００７２】

まず、要求元クライアントから送信されたクライアント識別情報を基に、登録情報データベースに保持されている該当クライアントのエントリを参照して、登録内容の変更可能回数が０であるかどうかを判断する（ステップＳ２１）。

【００７３】

変更可能回数が０ではない場合には、変更可能回数を１だけデクリメントした後（ステップＳ２２）、要求された登録内容の変更を行ない（ステップＳ２３）

、本処理ルーチンを成功終了する。

【００７４】

一方、変更可能回数が０である場合には、要求された登録の内容の変更を許可せず（ステップＳ２４）、本処理ルーチンを失敗終了する。

【００７５】

なお、変更可能回数はエンドユーザが改竄できないように保護されるものとする。例えば、記憶部１０２を内蔵するＣＰＵ１０１のように耐タンパ性のあるハードウェアを用いて、図８のような処理と変更可能回数の記憶をＣＰＵ１０１内部に保持し、チップ外部からの書換えを物理的に不可能にするなどの方法を用いる。

【００７６】

具体例（２）

登録済みの識別用情報を、別の装置又はユーザの識別用情報に置き換える頻度を制限する。

【００７７】

図９には、このような処理を実行することができるコンテンツ使用制御装置１００の変形例を模式的に示している。同図に示すように、このコンテンツ使用制御装置１００は、図１に示した装置構成に対し、さらに時間カウント機能を備えるタイマ部１０５が装備されている。あるいは、タイマ部１０５の代わりに、入力部１０４を介して他の装置（図示しない）から供給される時間情報を得る機能を備えるものであってもよい。

【００７８】

図１０には、図３に示した登録可能確認処理において、所定の時間内に１回だけ変更できるような制限を課すための処理手順をフローチャートの形式で示している。この処理手順は、実際には、ＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００７９】

所定の制限時間は、タイマにセットされる値とタイマのダウンカウント周期によって決まる。なお、タイマのカウンタは初期状態で０にセットされる。

【００８０】

まず、タイマのカウンタが既に０に到達しているかどうかを判別する（ステップＳ３１）。

【００８１】

タイマのカウンタ値がまだ０に到達していない場合には、登録内容の変更を不可にし（ステップＳ３２）、本処理ルーチンを失敗処理する。

【００８２】

一方、タイマのカウンタが０になっている場合には、タイマのカウンタに制限値をセットし（ステップＳ３３）、タイマのカウントダウンを開始し（ステップＳ３４）、登録内容の変更を許可して（ステップＳ３５）、本処理ルーチンを成功処理する。

【００８３】

タイマ動作時のカウンタ値には改竄保護がなされるものとする。例えば、タイマ機能を内蔵したＣＰＵ１０１を使うとか、定期的にタイマの値を読んでＣＰＵ１０１内のレジスタに記憶し、読んだ値と直前の記憶値を比較し、読んだ値の方が大きい場合は、記憶値をタイマにセットし直すなどの方法を用いる。

【００８４】

また、変更をキャンセルする場合は、タイマの初期化も行なわないという実装も考えられる。これを実現する場合は、最終的なキャンセル確認処理の後で、変更を行なう際にタイマの初期化も行なうことで対応することができる。

【００８５】

図１１には、図９及び図１０に示したようにタイマ機能を使用する代わりに、現在日時を用いることによって所定時間内の変更回数を制限するための処理手順をフローチャートの形式で示している。この処理手順は、実際には、ＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００８６】

まず、変更日時と現時点の間隔が制限時間以上かどうかを判別する（ステップＳ４１）。

【００８７】

変更日時と現時点の間隔が制限時間未満である場合には、登録内容の変更を不可とし（ステップＳ４２）、本処理ルーチンを失敗処理する。

【００８８】

一方、変更日時と現時点の間隔が制限時間以上である場合には、現時点を変更日時として記憶し（ステップＳ４３）、登録内容の変更を許可して（ステップＳ４４）、本処理ルーチンを成功処理する。

【００８９】

なお、現在日時を他の装置から得る場合は、共有する鍵で暗号化伝送したり、公開鍵暗号技術による電子署名を付けたりするなどの方法で改竄防止を行なうものとする。

【００９０】

具体例（４）

登録済みの識別用情報の置き換えに際して、所定の操作を要求する。例えば、パスワードの入力、所定のボタン押下操作（例えば、幾つかのボタンを決められた順序で押す）などである。

【００９１】

図１２には、図３に示した登録可能確認処理において、パスワード入力を要求するための処理手順をフローチャートの形式で示している。この処理手順は、実際には、ＣＰＵ１０１が所定のプログラム・コードを実行するという形態で実現される。

【００９２】

まず、入力部１０４を介してパスワードの入力処理を行ない（ステップＳ５１）、該入力されたパスワードが正しいかどうかを判別する（ステップＳ５２）。

【００９３】

パスワードが正しくない場合には、登録内容の変更を不可とし（ステップＳ５２）、本処理ルーチンを失敗処理する。

【００９４】

一方、パスワードが正しい場合には、登録内容の変更を許可して（ステップＳ５３）、本処理ルーチンを成功処理する。

【００９５】

なお、どんなパスワードが正当であるかは、あらかじめ記憶部１０２に保持しているものとする。図中のパスワードを所定の操作とすれば、ボタン押下操作に関する処理手続きになる。

【００９６】

具体例（５）

登録済みの識別用情報の置き換えに際して、他の装置又は管理者から変更許諾情報を得ることを要求する。例えば、パスワードや鍵データを電話、インターネット、郵便、記録媒体、口頭などによって得て、直接又は間接的に装置がそれを確認した段階で変更を可能にする。

【００９７】

図１３には、コンテンツ使用制御装置１００のユーザが変更許諾情報の発行者に対して、変更を可能にするパスワードを要求する処理のシーケンス例を示している。

【００９８】

ユーザは、装置の固有識別情報（例えば装置に刻印されているものとする）とともに、パスワード要求を送る。これに対し、発行者は得た装置識別情報と、自身が管理するパスワード・シリアル番号を基に、パスワードを作成する。

【００９９】

図１４には、パスワードの構成例を示している。同図に示す例では、パスワードは、装置識別情報と、パスワード・シリアル番号と、署名データで構成される。ここで、署名データは、例えば装置識別情報とパスワード・シリアル番号に対する公開鍵暗号技術に基づく電子署名などである。

【０１００】

ユーザは、受け取ったパスワードを装置に入力することで登録内容の変更操作を行なう。そして、コンテンツ使用制御装置１００側では、図１２に示したような処理手続きに従って、登録内容の変更の可否を判断する。

【０１０１】

図１５には、上述のようにして作成されたパスワードの正当判断の処理手順を

フローチャートの形式で示している。ここで、コンテンツ使用制御装置１００はあらかじめ記憶部１０２に署名データの検証に必要な情報（許可者の公開鍵など）と装置識別情報を保持し、パスワード・シリアル番号の記憶は初期状態で０を保持するものとする。

【０１０２】

まず、署名データが装置識別情報とパスワード・シリアル番号に対応しているかどうかを判別する（ステップＳ６１）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ６６）、本処理ルーチンを失敗終了する。

【０１０３】

次いで、パスワード内の装置識別情報があらかじめ記憶している値と一致するかどうかを判別する（ステップＳ６２）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ６６）、本処理ルーチンを失敗終了する。

【０１０４】

次いで、パスワード・シリアル番号が記憶する値より大きいかどうかを判別する（ステップＳ６３）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ６６）、本処理ルーチンを失敗終了する。

【０１０５】

一方、上述した判別結果がすべて肯定的である場合には、パスワード・シリアル番号の記憶内容を更新し（ステップＳ６４）、登録内容の変更を許可して（ステップＳ６５）、本処理ルーチンを成功終了する。

【０１０６】

このフロー処理により、パスワードを特定の装置だけで１回だけ使用できるようにすることができる。

【０１０７】

なお、上述した具体例（２）における回数管理や、具体例（３）における頻度管理を、家庭内などのエンドユーザ側に設置されているコンテンツ使用制御装置１００ではなく、パスワードの発行元で行なうという応用も考えられる。この場

合、パスワード発行元は、装置の識別情報別に、変更回数や変更日時を保持するデータベースを持ち、登録内容の変更を行なう度に図８乃至図１１にしめしたような処理手続きを実行することになる。

【０１０８】

また、具体例（２）～（５）で挙げた処理のうち２つ以上を組み合わせて実装することも考えられる。例えば、変更許諾を得る度に３回まで変更が可能という具合である。

【０１０９】

具体例（６）

登録の変更制限の制限内容を可変にする。例えば変更制限回数を有償のサービスで５回から１０回にするというようなことを可能にする。

【０１１０】

具体例（７）

登録の制限内容の変更に際して、他の装置又は所定の管理者から変更許諾情報を得ることを求める。例えば、パスワードや鍵データを電話、インターネット、郵便、記録媒体、口頭などによって得て、直接又は間接的に装置がそれを確認した段階で変更を可能にする。

【０１１１】

図１６には、コンテンツ使用制御装置１００のユーザが変更許諾情報の発行者に対して、変更を可能にするパスワードを要求する処理のシーケンス例を示している。

【０１１２】

ユーザは、装置の固有識別情報（例えば装置に刻印されているものとする）とともに、パスワード要求を送る。これに対し、発行者は得た装置識別情報と、自身が管理するパスワード・シリアル番号を基に、パスワードを作成する。

【０１１３】

図１７には、パスワードの構成例を示している。同図に示す例では、パスワードは、装置識別情報と、パスワード・シリアル番号と、登録変更の制限内容と、署名データで構成される。ここで、署名データは、例えば装置識別情報とパスワ

ード・シリアル番号に対する公開鍵暗号技術に基づく電子署名などである。

【０１１４】

ユーザは、受け取ったパスワードを装置に入力することで登録内容の変更操作を行なう。そして、コンテンツ使用制御装置１００側では、図１２に示したような処理手続きに従って、登録内容の変更の可否を判断する。

【０１１５】

図１８には、上述のようにして作成されたパスワードの正当判断の処理手順をフローチャートの形式で示している。ここで、コンテンツ使用制御装置１００はあらかじめ記憶部１０２に署名データの検証に必要な情報（許可者の公開鍵など）と装置識別情報を保持し、パスワード・シリアル番号の記憶は初期状態で０を保持するものとする。

【０１１６】

まず、署名データが装置識別情報とパスワード・シリアル番号に対応しているかどうかを判別する（ステップＳ７１）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ７６）、本処理ルーチンを失敗終了する。

【０１１７】

次いで、パスワード内の装置識別情報があらかじめ記憶している値と一致するかどうかを判別する（ステップＳ７２）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ７６）、本処理ルーチンを失敗終了する。

【０１１８】

次いで、パスワード・シリアル番号が記憶する値より大きいかどうかを判別する（ステップＳ７３）。この判別結果が否定的である場合には、登録内容の変更を不許可にし（ステップＳ７６）、本処理ルーチンを失敗終了する。

【０１１９】

一方、上述した判別結果がすべて肯定的である場合には、パスワード・シリアル番号の記憶内容を更新し（ステップＳ７４）、登録の変更制限を制限内容に更新可して（ステップＳ７５）、本処理ルーチンを成功終了する。

【０１２０】

具体例（８）

登録情報は変更せずに、登録された他の装置又はユーザによる所定サービスの利用の許可／不許可を制御可能にする。

【０１２１】

このような場合、万一、登録した装置が盗難、紛失して他人の手に渡った場合などに、サービスの利用を禁止することで、不正利用を停止することができる。

【０１２２】

例えば図７に示したように、個々の登録装置又はユーザに対する無効フラグをユーザに設定できるようにし、コンテンツ使用制御装置１００がこれを参照して利用の許可制御をすることで実現できる。

【０１２３】

［追補］

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２４】

【発明の効果】

以上詳記したように、本発明によれば、ネットワークなどを経由して取得されたコンテンツに関する使用を特定のサーバ管理者の下で制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することができる。

【０１２５】

また、本発明によれば、エンドユーザの管理下に置かれるコンテンツの不正な使用を制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することができる。

【０１２６】

また、本発明によれば、コンテンツがホーム・ネットワークなどのエンドユーザの管理下に置かれる際に、所定の使用条件を越えて無制限にコンテンツが配信・流通されることがないように制御することができる、優れたコンテンツ使用制御装置及びコンテンツ使用制御方法、並びにコンピュータ・プログラムを提供することができる。

【０１２７】

本発明は、例えば映画や音楽などの有料コンテンツを出力可能な装置が、そのコンテンツの利用者を制限することで、そのコンテンツの利用権限を持たないユーザによる不正利用を防ぐのに有効である。

【０１２８】

まず、本発明に係るコンテンツ使用制御装置は、その提供サービスの利用に先立って利用する装置又はユーザの識別情報を登録する必要がある。これにより、登録ができない装置及びユーザによる不正利用を排除することができる。

【０１２９】

さらに、本発明の係るコンテンツ使用制御装置のユーザが故意にサービスの利用権限のない装置又はユーザを登録しても、その変更は制限されているため、無制限な不正利用はできない。また、他ユーザやその装置を登録してしまうと、自身や家族による利用を妨げる可能性があることから、変更の制限は不正登録を抑制する効果も期待できる。

【０１３０】

一方、このようにサービスの利用制限を設けることで、無制限な不正利用を防止できるため、コンテンツ提供者の要求を十分満たすこととなり、さまざまなサービス、コンテンツが利用できるようになることが期待される。

【０１３１】

また、登録済み情報の置き換え制限を変えられるようにすることで、エンドユーザが不都合を感じないレベルに制限を緩和するオプションを得ることが可能になるとともに、サービスやコンテンツの権利者は潜在的な不正利用可能範囲をコントロールすることができる。

【図面の簡単な説明】

【図１】

本発明の実施に供されるコンテンツ使用制御装置１００の基本構成を模式的に示した図である。

【図２】

コンテンツ使用制御装置１００（サーバ）が他の装置やユーザ（クライアント）に対して行なう登録処理シーケンスを示した図である。

【図３】

コンテンツ使用制御装置１００上で実行される登録処理の手順を示したフローチャートである。

【図４】

サーバとしてのコンテンツ使用制御装置１００に対して他の装置やユーザ（クライアント）がサービス要求を行なうための動作シーケンスを示した図である。

【図５】

コンテンツ使用制御装置１００がサービス提供に際して行なうサービス可否判定処理の手順を示したフローチャートである。

【図６】

サービス要求シーケンス内でクライアントの登録処理まで行なうようにした場合の動作シーケンスを示した図である。

【図７】

コンテンツ使用制御装置１００が保持する登録情報データベースの構成例を示した図である。

【図８】

登録内容の変更可能確認の処理手順を示したフローチャートである。

【図９】

別の装置又はユーザの識別用情報に置き換える頻度を制限する処理を実行することができるコンテンツ使用制御装置１００の変形例を模式的に示した図である。

【図１０】

図３に示した登録可能確認処理において、所定の時間内に１回だけ変更できる

ような制限を課すための処理手順を示したフローチャートである。

【図１１】

現在日時を用いることによって所定時間内の変更回数を制限するための処理手順を示したフローチャートである。

【図１２】

図３に示した登録可能確認処理において、パスワード入力を要求するための処理手順を示したフローチャートである。

【図１３】

コンテンツ使用制御装置１００のユーザが変更許諾情報の発行者に対して、変更を可能にするパスワードを要求する処理のシーケンス例を示した図である。

【図１４】

パスワードの構成例を示した図である。

【図１５】

パスワードの正当判断の処理手順を示したフローチャートである。

【図１６】

コンテンツ使用制御装置１００のユーザが変更許諾情報の発行者に対して、変更を可能にするパスワードを要求する処理のシーケンス例を示した図である。

【図１７】

パスワードの構成例を示した図である。

【図１８】

パスワードの正当判断の処理手順を示したフローチャートである。

【符号の説明】

１００…コンテンツ使用制御装置

１０１…ＣＰＵ

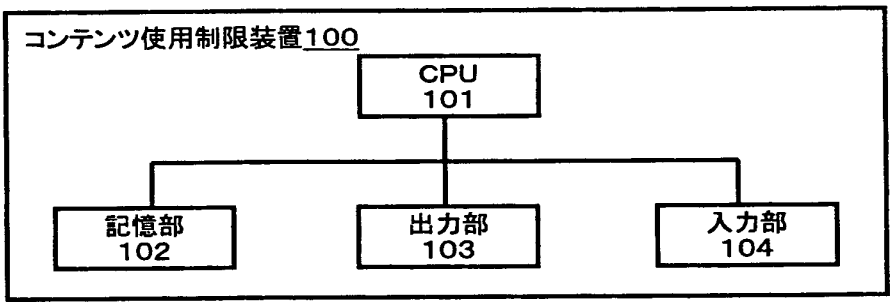
１０２…記憶部

１０３…出力部

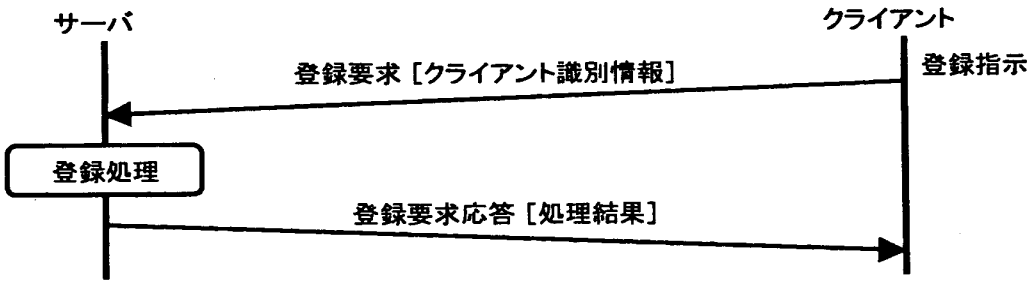
１０４…入力部

【書類名】　　図面

【図１】

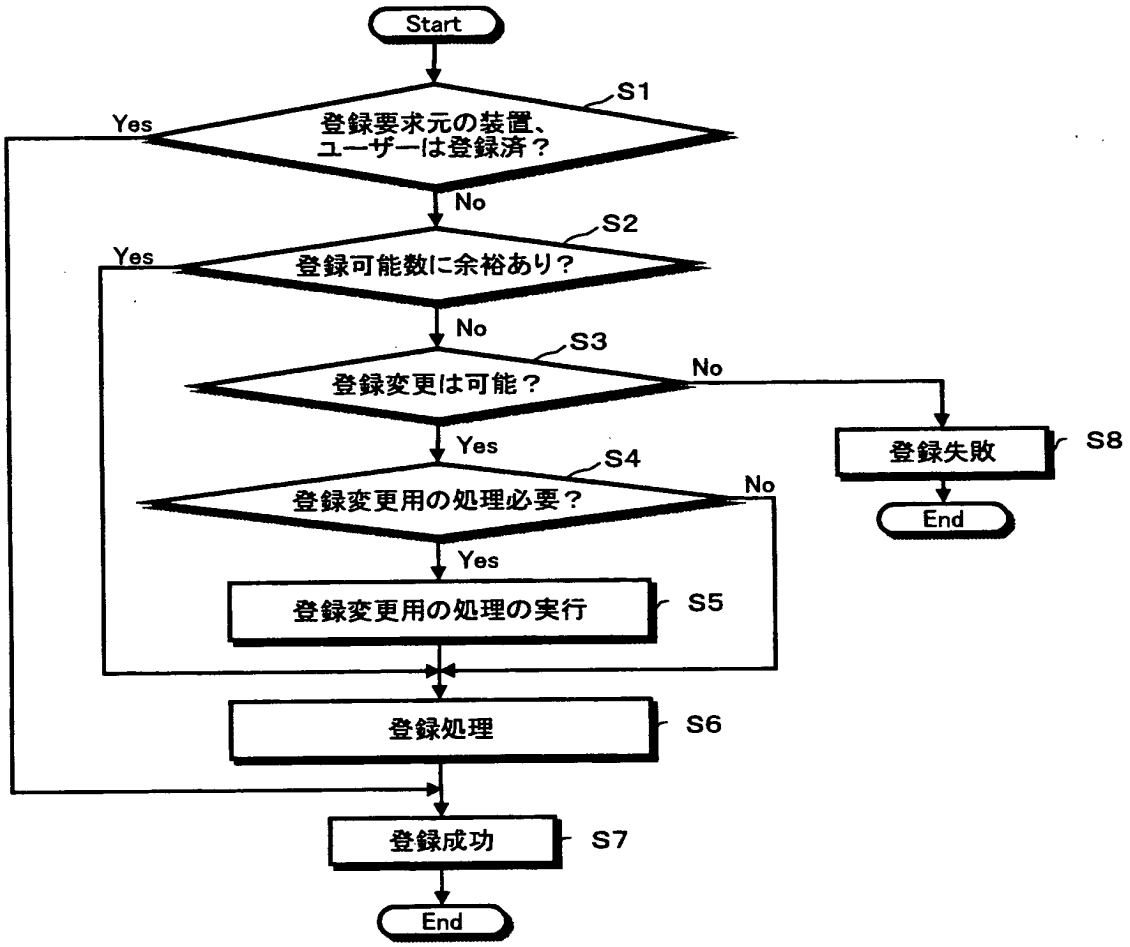


【図２】

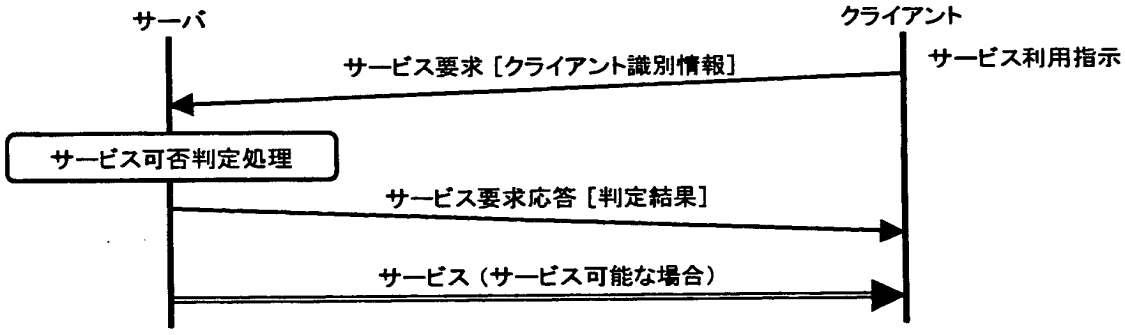


出証特２００３－３０５０９９４

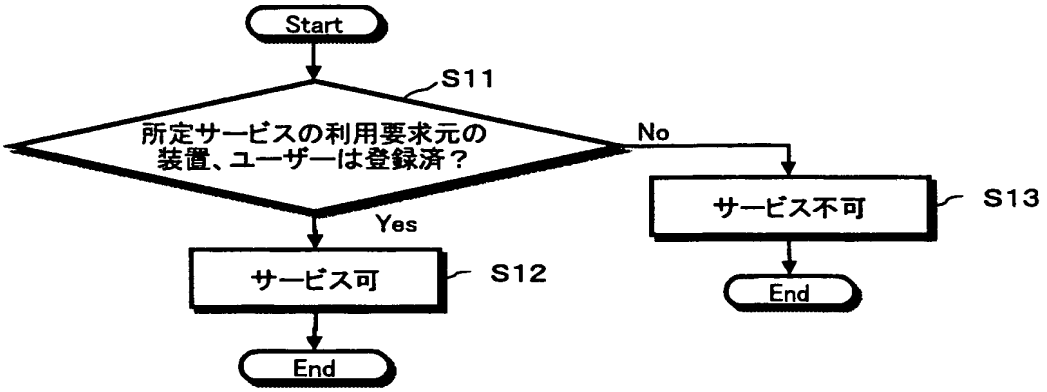
【図３】


Start
S1
登録要求元の装置、
ユーザーは登録済？
Yes
No
S2
登録可能数に余裕あり？
Yes
No
S3
登録変更は可能？
No
登録失敗
S8
End
Yes
S4
登録変更用の処理必要？
No
Yes
登録変更用の処理の実行
S5
登録処理
S6
登録成功
S7
End

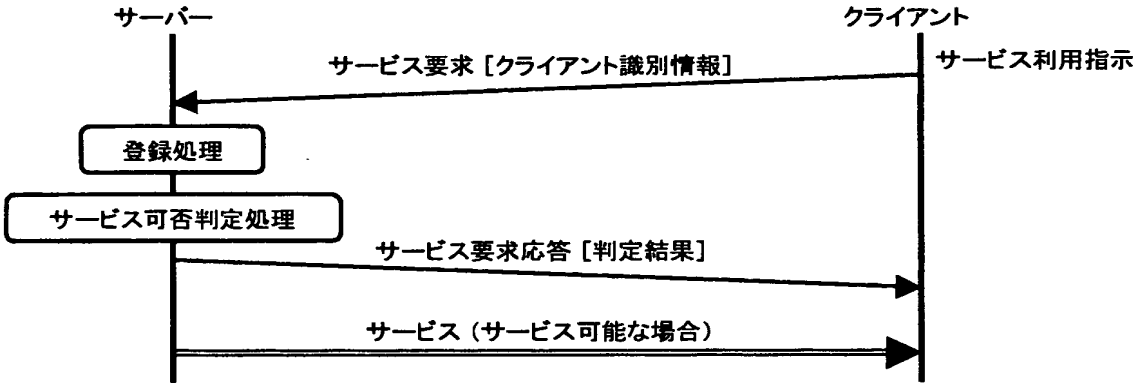
【図４】


サーバ
クライアント
サービス要求［クライアント識別情報］
サービス利用指示
サービス可否判定処理
サービス要求応答［判定結果］
サービス（サービス可能な場合）

【図５】



【図６】

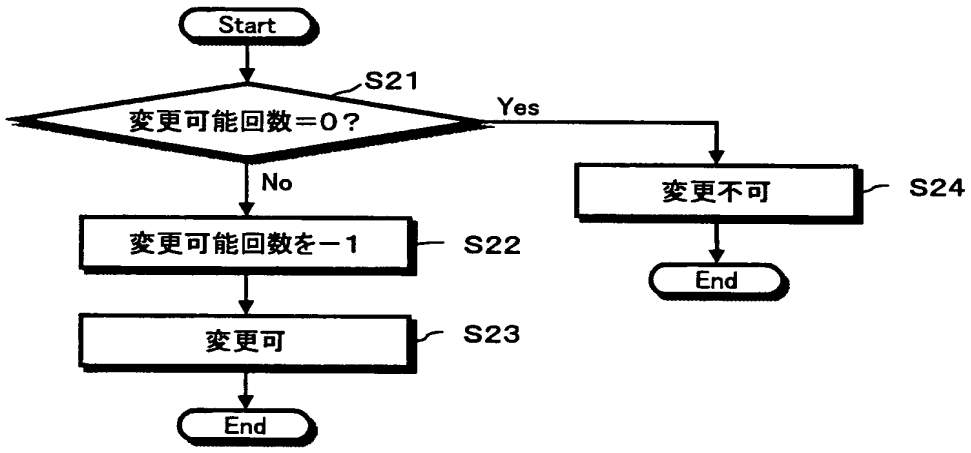


出証特２００３－３０５０９９４

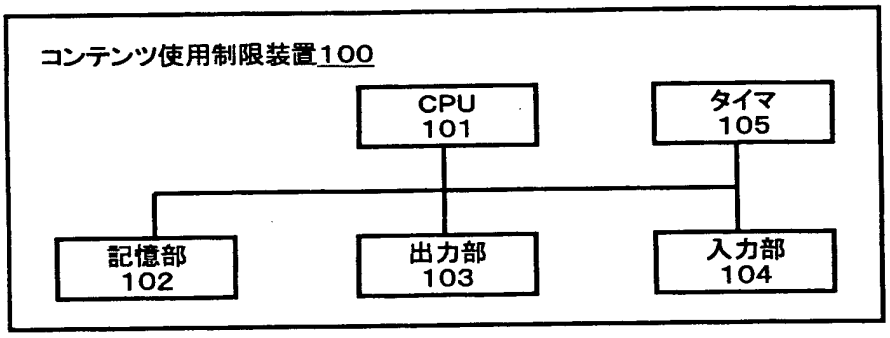
【図７】

新規登録可能数	
無効フラグ	クライアント識別情報＃1
無効フラグ	クライアント識別情報＃2
無効フラグ	クライアント識別情報＃3
：	：
無効フラグ	クライアント識別情報＃n

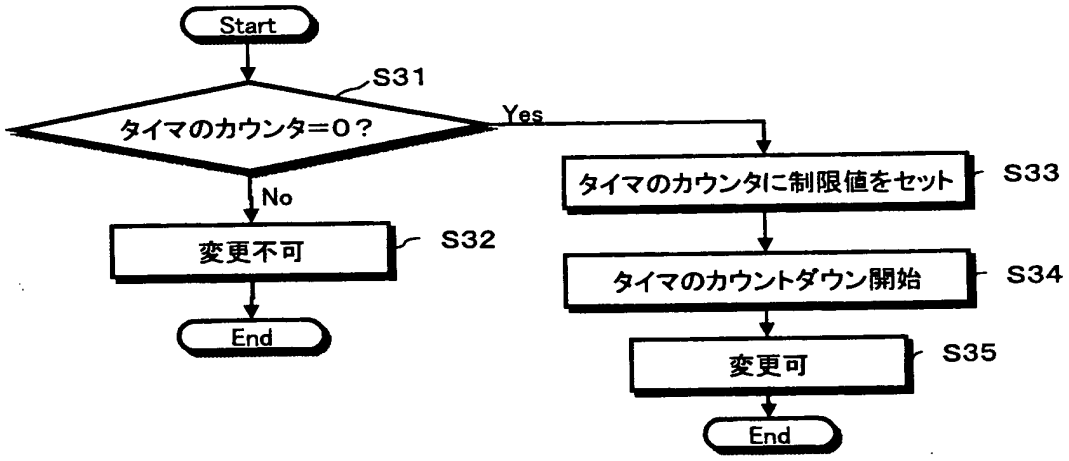
【図８】



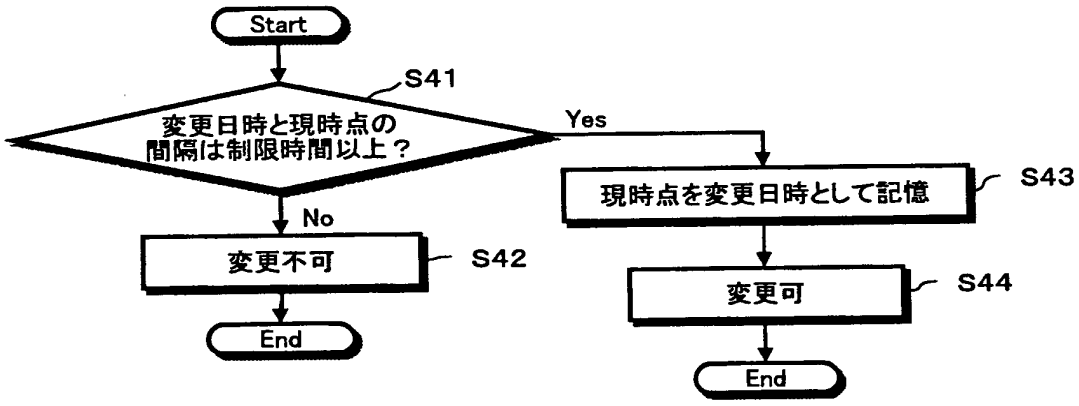
【図９】


コンテンツ使用制限装置100
CPU
101
タイマ
105
記憶部
102
出力部
103
入力部
104

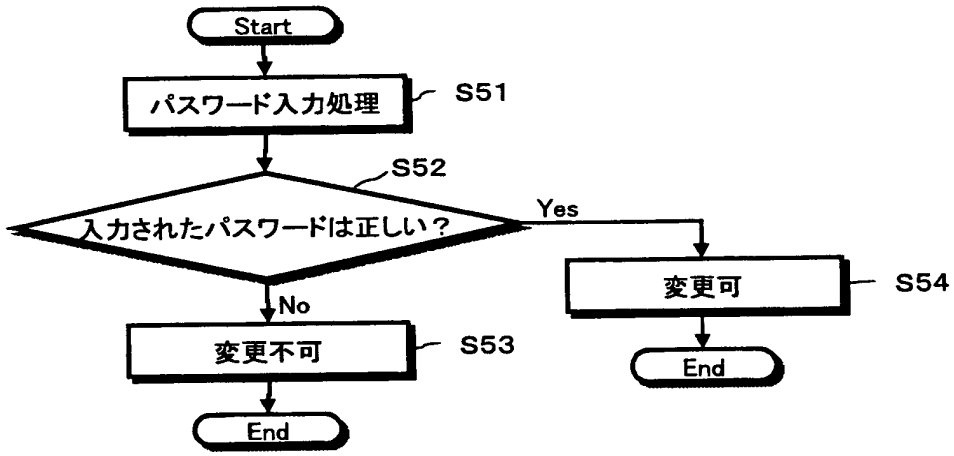
【図１０】


Start
S31
タイマのカウンタ＝０？
Yes
No
変更不可
S32
End
タイマのカウンタに制限値をセット
S33
タイマのカウントダウン開始
S34
変更可
S35
End

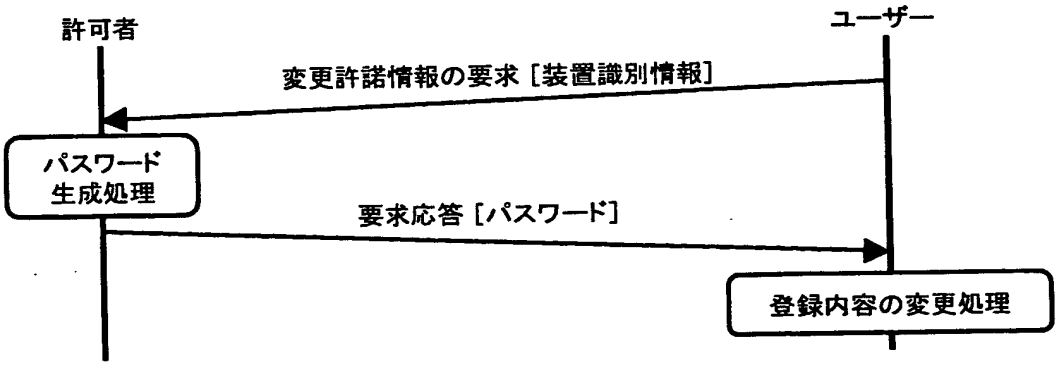
【図１１】


Start
S41
変更日時と現時点の
間隔は制限時間以上？
Yes
No
現時点を変更日時として記憶
S43
変更不可
S42
変更可
S44
End
End

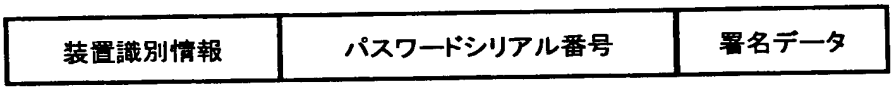
【図１２】


Start
パスワード入力処理
S51
S52
入力されたパスワードは正しい？
Yes
No
変更可
S54
変更不可
S53
End
End

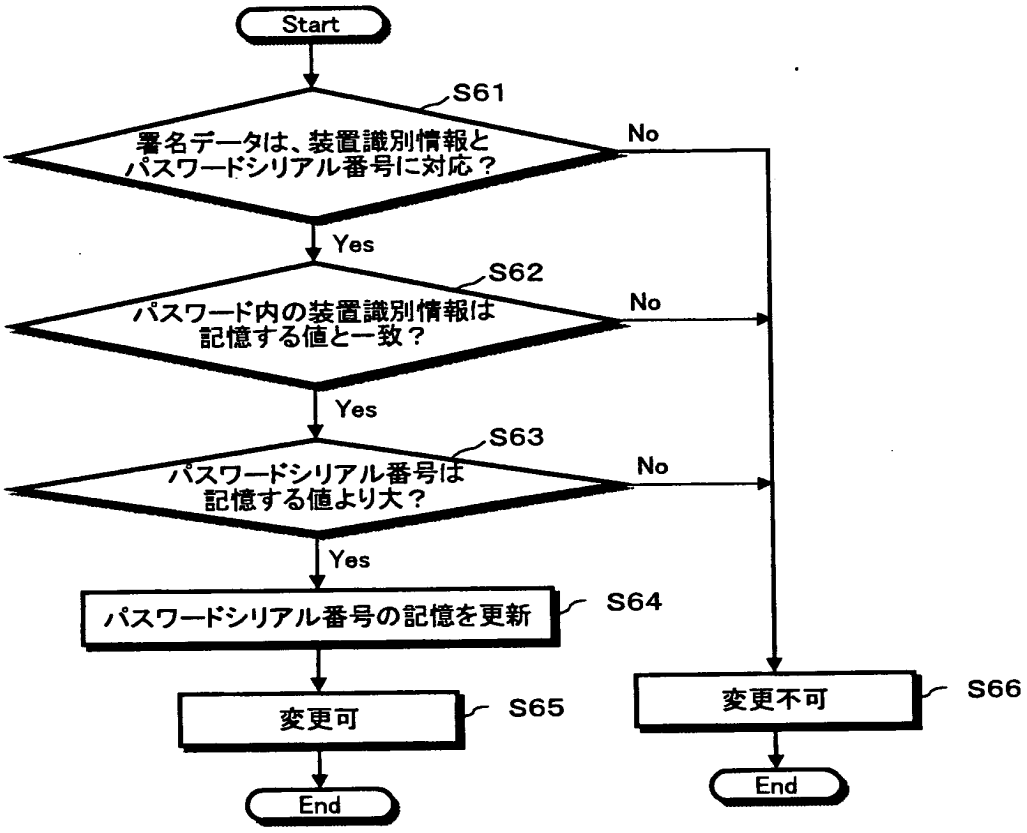
【図１３】


許可者
ユーザー
変更許諾情報の要求［装置識別情報］
パスワード
生成処理
要求応答［パスワード］
登録内容の変更処理

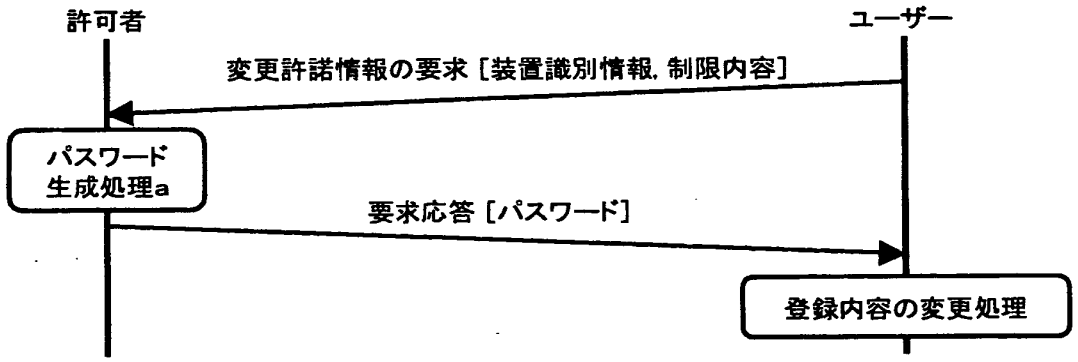
【図１４】


装置識別情報
パスワードシリアル番号
署名データ

【図１５】


Start
S61
署名データは、装置識別情報と
パスワードシリアル番号に対応？
No
Yes
S62
パスワード内の装置識別情報は
記憶する値と一致？
No
Yes
S63
パスワードシリアル番号は
記憶する値より大？
No
Yes
パスワードシリアル番号の記憶を更新
S64
変更可
S65
End
変更不可
S66
End

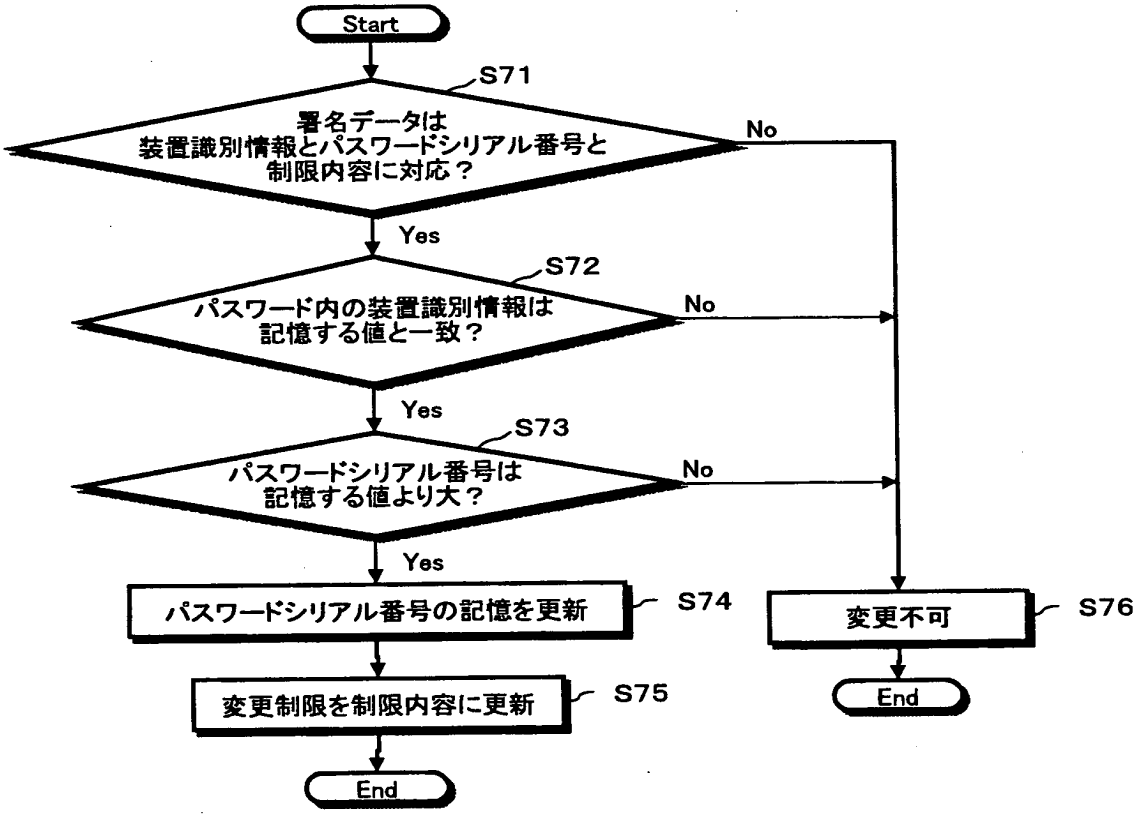
【図１６】



【図１７】

装置識別情報	パスワードシリアル番号	制限内容	署名データ

【図１８】


Start
S71
署名データは
装置識別情報とパスワードシリアル番号と
制限内容に対応？
No
Yes
S72
パスワード内の装置識別情報は
記憶する値と一致？
No
Yes
S73
パスワードシリアル番号は
記憶する値より大？
No
Yes
パスワードシリアル番号の記憶を更新
S74
変更制限を制限内容に更新
S75
End
変更不可
S76
End

【書類名】　要約書

【要約】

【課題】　エンドユーザの管理下に置かれるコンテンツの不正な使用を制御する。

【解決手段】　コンテンツ使用制御装置は、サービスを提供する際、そのサービスが正当な提供先以外の装置やユーザから無制限に使用されることがないように、提供先の装置やユーザを登録・確認する機能を備え、さらに登録内容の書き換えを制限する機能を持つ。これらの制限を与えることで、サービスに供される情報の著作権保護を実現する。装置の具体例は映画や音楽などのコンテンツを保持するサーバであり、クライアント（携帯電話やサーバに接続されるＴＶやＰＣなど）やユーザの要求に応じて、コンテンツを供給するシステムに適用される。

【選択図】　図１

出証特２００３－３０５０９９４

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社

２．変更年月日　　２００３年　５月１５日
［変更理由］　名称変更
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社